6.3 Responding to Security Incidents

GTA Georgia Technology Authority

Incident Response Standards

STANDARD NUMBER: 6.3.1	EFFECTIVE DATE: July 1, 2005

PURPOSE

To implement a security incident response and reporting process and train employees on how to use the process.

SCOPE

This standard set forth the requirements for response and reporting in case of security breach incidents on all State of Georgia information systems networks.

POLICY

Each agency shall implement a security incident response and reporting process and train its employees on how to use the process.

INCIDENT RESPONSE STANDARD

1. **Agencies must have a documented incident response capability**
2. **Agencies must have a designated incident lead**
3. **Agencies must report criminal incidents to the Georgia Cybercrime Task Force**

TERMS AND DEFINITIONS

- **Computer Security Incident --** An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- **Criminal Incident** – The downloading or accessing Child pornography or any other criminal activity
- **Background Noise –**
  - General broadcast spam
  - In-bound traffic blocked at firewall that does not appear to be a target
  - Occasional virus/worm infection of one or two PC's with minimal cleanup required
  - Ad-ware that does not have major side effects on one or two PC's
- Event of Interest
  - In-bound traffic blocked at firewall that appears to be a directed attack

    - Cluster of several PC's infected with the same virus/worm, but still requiring minimal cleanup
    - Excessive or targeted spam leaking past existing filters
    - Ad-Ware that affects normal machine operation or contains spy ware
    - Novel or directed Phishing attack to agency employees
    - Inadvertent unintentional infraction of accepted policy
- Event of Concern
    - Direct attack on firewall itself, but without success
    - Large virus/worm infection or propagation by new vector
    - Internally propagating virus/worm
    - Repeated or serious infractions of accepted use policy
    - Downloading or accessing adult pornography
- Security Incident
    - Penetration of firewall
    - Compromise of any server, including Web server defacement
    - Compromise on loss of data on server
    - Infractions of accepted use policy that are flagrant or extreme
    - External propagation of virus/worm

GUIDELINES

Please see NIST Document 800-61, Computer Security Incident Handling Guide. This document can be found in PDF and zipped PDF formats at:

`http://csrc.nist.gov/publications/nistpubs/`